

Democratizing AI scientists using ToolUniverse

Shanghua Gao¹, Richard Zhu^{1,2,*}, Pengwei Sui^{1,*}, Zhenglun Kong^{1,*}, Sufian Aldogom^{1,*}, Yepeng Huang¹,
Ayush Noori¹, Reza Shamji^{1,2}, Krishna Parvataneni³, Theodoros Tsiligkaridis⁴, Marinka Zitnik^{1,5,6,7,‡}

¹Department of Biomedical Informatics, Harvard Medical School, Boston, MA

²Harvard College, Harvard University, Cambridge, MA

³Massachusetts Institute of Technology, Cambridge, MA

⁴MIT Lincoln Laboratory, Lexington, MA

⁵Kempner Institute for the Study of Natural and Artificial Intelligence, Harvard University, Cambridge, MA

⁶Broad Institute of MIT and Harvard, Cambridge, MA

⁷Harvard Data Science Initiative, Cambridge, MA

* Co-second authors

‡ Correspondence: marinka@hms.harvard.edu

TOOLUNIVERSE web service is at <https://aiscientist.tools>

TOOLUNIVERSE code is at <https://github.com/mims-harvard/ToolUniverse>

TOOLUNIVERSE package is at <https://pypi.org/project/tooluniverse>

AI scientists are emerging computational systems that serve as collaborative partners in discovery. These systems remain difficult to build because they are bespoke, tied to rigid workflows, and lack shared environments that unify tools, data, and analyses into a common ecosystem. In genomics, unified ecosystems have transformed research by enabling interoperability, reuse, and community-driven development; AI scientists require comparable infrastructure. We present TOOLUNIVERSE, an ecosystem for building AI scientists from any language or reasoning model across open- and closed-weight models. TOOLUNIVERSE standardizes how AI scientists identify and call tools by providing more than 600 machine learning models, datasets, APIs, and scientific packages for data analysis, knowledge retrieval, and experimental design. It automatically refines tool interfaces for correct use by AI scientists, generates new tools from natural language descriptions, iteratively optimizes tool specifications, and composes tools into agentic workflows. In a case study of hypercholesterolemia, TOOLUNIVERSE was used to create an AI scientist to identify a potent analog of a drug with favorable predicted properties. The open-source TOOLUNIVERSE is available at <https://aiscientist.tools>.

Main

AI scientists hold promise as computational systems that can reason, experiment, and collaborate in discovery [1]. Yet most require one-off implementation, remain constrained by rigid workflows, and lack shared environments for reuse and growth [2, 3]. In contrast, fields such as genomics have advanced through ecosystems that integrate tools and standardized analyses [4–8]. Comparable infrastructure is needed to support AI scientists [9]. Here we introduce TOOLUNIVERSE, a general ecosystem for constructing AI scientists at scale by combining large language models

(LLMs), AI agents, and large reasoning models (LRMs) with scientific tools, including machine learning models, bioinformatics workflows, retrieval systems, remote and local datasets, scientific packages for data analysis, visualization and lab automation, and human-in-the-loop and safety tools (Figure 1a). As scientific research requires interaction with the real world rather than text-based reasoning alone [1, 10], TOOLUNIVERSE implements an environment where AI models can invoke tools, run experiments, and incorporate feedback from human experts or computational models. This environment wraps around a user-specified AI model, such as LLM, AI agent, or LRM, to create a customized AI research assistant (i.e., an AI scientist) tailored to user instruction without additional model training or fine-tuning.

TOOLUNIVERSE includes more than 600 tools spanning machine learning models, agents, software packages, robotics, datasets, and remote endpoints such as APIs and knowledge bases (Figure 1b). AI models face challenges in selecting and using these tools effectively, yet being able to use tools is essential for autonomous scientific research [2]. Scientific tools differ in purpose and complexity, from molecular docking predictors to literature retrieval APIs, and often require distinct input formats and parameters. Many are multimodal, processing genomic sequences, protein structures, microscopy images, or clinical text, while others perform Python-based modeling or statistical analyses that depend on specific runtime environments. Some operate locally, whereas others run remotely through APIs or laboratory automation systems. Overlapping and redundant functionalities between tools mean that each tool must be precisely described so that AI scientists can select and invoke the right ones for a given task.

To address these compatibility issues of AI scientists using tools and making the large toolbox in TOOLUNIVERSE available for effective use by AI scientists, analogous to the role of HTTP in regulating internet communication (Figure 1c), *AI-tool interaction protocol* in TOOLUNIVERSE governs how AI scientists issue tool requests and receive results of executing the tools. The protocol implements two operations (Figure 1d) in TOOLUNIVERSE: *Find Tool*, which maps natural language descriptions of tools to tool specifications that are understood by the underlying AI model that powers the AI scientist, and *Call Tool*, which executes a selected tool with arguments and returns the result, such as text, embeddings, or JSON objects.

TOOLUNIVERSE is continually expanded with new tools. New tools can be registered locally or remotely and integrated without additional configuration [11]. Tools with complex dependencies or restricted access are supported through remote connections. As we describe below, TOOLUNIVERSE creates new tools from natural language descriptions, optimizes tool specifications itera-

tively, and composes interoperable tools. It chains tools for sequential or parallel execution so that AI scientists built with TOOLUNIVERSE can orchestrate workflows in a self-directed manner.

The TOOLUNIVERSE Ecosystem

At the core of TOOLUNIVERSE is the AI-tool interaction protocol that defines tools and standardizes how AI scientist systems interact with them. This protocol comprises three elements: a specification schema, an interaction schema, and communication methods. The specification schema provides a common format for describing each tool’s function, parameters, and outputs, enabling any client (whether an LLM, agent, or human user) to invoke tools without knowledge of their internal implementation. The interaction schema defines requests in a uniform way, encoding function calls with tool names and arguments. This standardization makes diverse tools interchangeable, whether they are local functions, remote machine learning models, or laboratory instruments. Communication protocols manage execution. Local operations run directly in Python, while remote serving uses the Model Context Protocol (MCP) [11] to transmit requests across networks. These abstractions make heterogeneous tools accessible to AI scientists through a consistent and extensible protocol.

Components of TOOLUNIVERSE

TOOLUNIVERSE is powered by core components that enable tool discovery, execution, integration, composition, optimization, and creation. These components support the lifecycle of AI scientists.

Tool Finder (Figure 1e). The Tool Finder identifies relevant tools from more than 600 tools using three strategies: keyword search for rapid retrieval, LLM-based in-context search for semantic understanding, and embedding search for scalable similarity matching. By flexibly identifying tools relevant to a user-specified task, TOOLUNIVERSE allows AI scientists built within the ecosystem to efficiently locate and execute task-relevant tools.

Tool Caller (Figure 1f). The tool caller executes selected tools through the TOOLUNIVERSE interaction protocol or via MCP requests. It validates inputs against tool specifications, dynamically loads tools on demand, and returns structured outputs, enabling reliable and efficient execution across heterogeneous resources.

Tool Manager (Figure 1g). The tool manager integrates local and remote tools through standardized registration. Local tools are added directly with lightweight specifications, while remote tools, including those with specialized dependencies or privacy constraints, connect via the MCP. This

approach makes tools function as interchangeable components within the same ecosystem.

Tool Composer (Figure 1h). The tool composer constructs composite tools by chaining or orchestrating existing ones. It supports sequential, parallel, and feedback-driven execution, enabling adaptive workflows. For example, it can run multiple literature searches in parallel and then invoke a summarization agent, illustrating how tools can be combined into agentic loops for multi-step analysis [12, 13].

Tool Discoverer (Figure 1i). Tool Discoverer generates new tools from natural language descriptions. It synthesizes formal specifications, produces executable implementations, validates outputs, and iteratively refines quality. This component ensures that newly created tools are maintainable and can be integrated into TOOLUNIVERSE.

Tool Optimizer (Figure 1j). The tool optimizer improves existing tool specifications through iterative refinement. By generating test cases, analyzing executions, and applying feedback from the analyzer agentic tool, it increases usability and removes redundancy in the descriptions of the tool specifications. Optimized specifications increase the composability of tools and ensure the correct use of tools across tasks.

Building AI Scientists with TOOLUNIVERSE

TOOLUNIVERSE integrates with LLMs, reasoning models, and agents to create customized AI scientists capable of planning, selecting tools, running experiments, and refining hypotheses. Setup requires only three steps: installing TOOLUNIVERSE, connecting it to a user-chosen AI model, and providing the model with a scientific problem. Once configured, the AI scientist can identify relevant tools, execute them, interpret results, and request human feedback when needed.

Three main approaches illustrate how TOOLUNIVERSE supports both general-purpose and specialized AI scientists. First, LLMs such as Claude or GPT can be equipped with tool access through simple in-context instructions [14] or a lightweight configuration, enabling them to invoke and chain tools during reasoning (Figure 2a). Second, agentic systems such as Gemini CLI can directly use TOOLUNIVERSE’s MCP server and Tool Finder to identify and call tools, requiring minimal user setup (Figure 2b). Third, specialized agents such as TxAgent for medical research [13], Virtual Lab for nanobody design [15], and GeneAgent for gene set function discovery [16] can use tools from TOOLUNIVERSE during training to improve tool use and reasoning [17] or during inference to expand their capabilities [18]. In the former case, reinforcement learning enables effective multi-tool collaborative reasoning [19, 20] (Figure 2c).

Therapeutic Discovery Case Study

Figure 2c shows how TOOLUNIVERSE can be applied to therapeutic discovery for hypercholesterolemia by connecting TOOLUNIVERSE with Gemini CLI to create an AI scientist system. The process begins with protein target identification [21, 22]: using its literature-mining, target-profiling, and tissue expression analysis tools, TOOLUNIVERSE prioritizes HMG-CoA reductase as the most promising candidate while documenting the potential side effects of targeting this enzyme. Then, the AI scientist uses TOOLUNIVERSE to access the DrugBank database and profile existing drugs that target HMG-CoA reductase. This results in the selection of lovastatin as the initial treatment to optimize due to its off-target effects.

Next, the AI scientist invokes *in silico* screening to evaluate existing drugs and novel small molecules [23]. TOOLUNIVERSE integrates structural analog retrieval from ChEMBL with predictive ML models, including Boltz-2 [24] for binding affinity and ADMET-AI [25] for pharmacological profiling. This combined workflow assesses binding probability, predicted affinity, and blood-brain barrier (BBB) penetrance across candidate compounds. The AI scientist then assesses the novelty of top candidates using patent-mining tools.

Through this screening process, the AI scientist identifies pravastatin, a drug with lower off-target effects than lovastatin [26]. In addition to reproducing established findings, TOOLUNIVERSE identifies a new candidate molecule (ChEMBL2347006/ChEMBL3970138) predicted to bind with higher affinity to HMG-CoA reductase, exhibit reduced blood-brain barrier penetrance, and display improved oral bioavailability and metabolic stability compared with lovastatin. Subsequent evidence confirmed that this compound had been patented for cardiovascular indications. The predicted binding affinity, binding likelihood, and BBB penetrance for all candidates are reported in Table 3. Using TOOLUNIVERSE, the AI scientist system selected, chained, and executed domain-specific tools to progress from hypothesis generation to candidate validation, while incorporating human feedback where needed. The workflow produced two candidates: an FDA-approved statin (pravastatin) and a patented small molecule. Both address lovastatin’s off-target effects due to activity outside the liver, one of its primary safety issues. The patented small molecule also has higher predicted binding affinity than lovastatin, suggesting greater potency.

Discussion

TOOLUNIVERSE moves beyond bespoke AI agents by providing an ecosystem for constructing AI scientists. It integrates tools and operations into workflows and incorporates automatic tool

discovery and optimization. These capabilities extend any language model, agent, or reasoning model with research functionality tailored to the user: models can retrieve data or run existing scripts, and also identify relevant analysis tools, execute them with user inputs, combine outputs into multi-step workflows, and iteratively refine or even generate new tools when gaps are encountered. It is applicable across scientific domains, and its integration of human-in-the-loop tools provides safeguards against erroneous outputs. For example, an AI scientist might propose several candidate compounds, and a human expert could validate tissue-specific expression before advancing them. Looking ahead, TOOLUNIVERSE will be used to build AI scientists for discovery and serve as a testbed to evaluate their integration with laboratory systems, potential for safety and biosecurity risks [27], and adherence to safeguards [28] and governance specifications [29].

TOOLUNIVERSE goes beyond orchestration frameworks such as GPT Agent [30], Gemini CLI [31], Claude Code [32], Qwen Code [33], LangChain [34], Haystack [35], Autogen [36] or CAMEL [37], and communication protocols like MCP [11] and AutoTools [38], which standardize how models access data resources, browsers, and tools. These systems are designed to route queries or connect agents with pre-defined tools, but they do not support the end-to-end lifecycle of creating, refining, and integrating tools into scientific workflows. In contrast, TOOLUNIVERSE can create and optimize tools and integrate them into agentic workflows beyond providing static tool registries. It introduces Tool Discoverer, which generates new tools from natural language descriptions and transforms them into ready-to-use components, and Tool Optimizer, which iteratively improves tool specifications through feedback from users and other AI systems. These capabilities enable TOOLUNIVERSE to manage and compose existing tools (Figure 1b) into new tools.

To ensure that tools can be effectively used by AI models to build AI scientists, TOOLUNIVERSE employs a multi-step validation process combining tool-specific test cases for each tool added to TOOLUNIVERSE, human expert reviews of input-output traces, and automated optimization of tool specifications to verify correctness and usability by AI scientists. Regular maintenance and a bug-reporting system further sustain long-term reliability.

A close parallel to TOOLUNIVERSE is the emergence of computational platforms in genomics, which created shared infrastructure for reuse, reproducibility, and open science innovation. TOOLUNIVERSE provides a comparable foundation for AI scientists, lowering barriers to their development and use in research.

Data and code availability. The project page and web service of TOOLUNIVERSE are at <https://aiscientist.tools>. The code, docs, and demos of TOOLUNIVERSE are at <https://github.com/mims-harvard/ToolUniverse>. The Python package of TOOLUNIVERSE is at <https://pypi.org/project/tooluniverse>. The therapeutic case study is at https://zitniklab.hms.harvard.edu/ToolUniverse/tutorials/tooluniverse_case_study.html.

Acknowledgments. We thank Nicholas Yang and Yuchang Su for their contributions to TOOLUNIVERSE. We gratefully acknowledge the support of NIH R01-HD108794, NSF CAREER 2339524, U.S. DoD FA8702-15-D-0001, ARPA-H Biomedical Data Fabric (BDF) Toolbox Program, Harvard Data Science Initiative, Amazon Faculty Research, Google Research Scholar Program, AstraZeneca Research, Roche Alliance with Distinguished Scientists (ROADS) Program, Sanofi iDEA-iTECH Award, GlaxoSmithKline Award, Boehringer Ingelheim Award, Merck Award, Optum AI Research Collaboration Award, Pfizer Research, Gates Foundation (INV-079038), Chan Zuckerberg Initiative, John and Virginia Kaneb Fellowship at Harvard Medical School, Biswas Computational Biology Initiative in partnership with the Milken Institute, Harvard Medical School Dean's Innovation Fund for the Use of Artificial Intelligence, and the Kempner Institute for the Study of Natural and Artificial Intelligence at Harvard University. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funders.

Competing interests. The authors declare no competing interests.

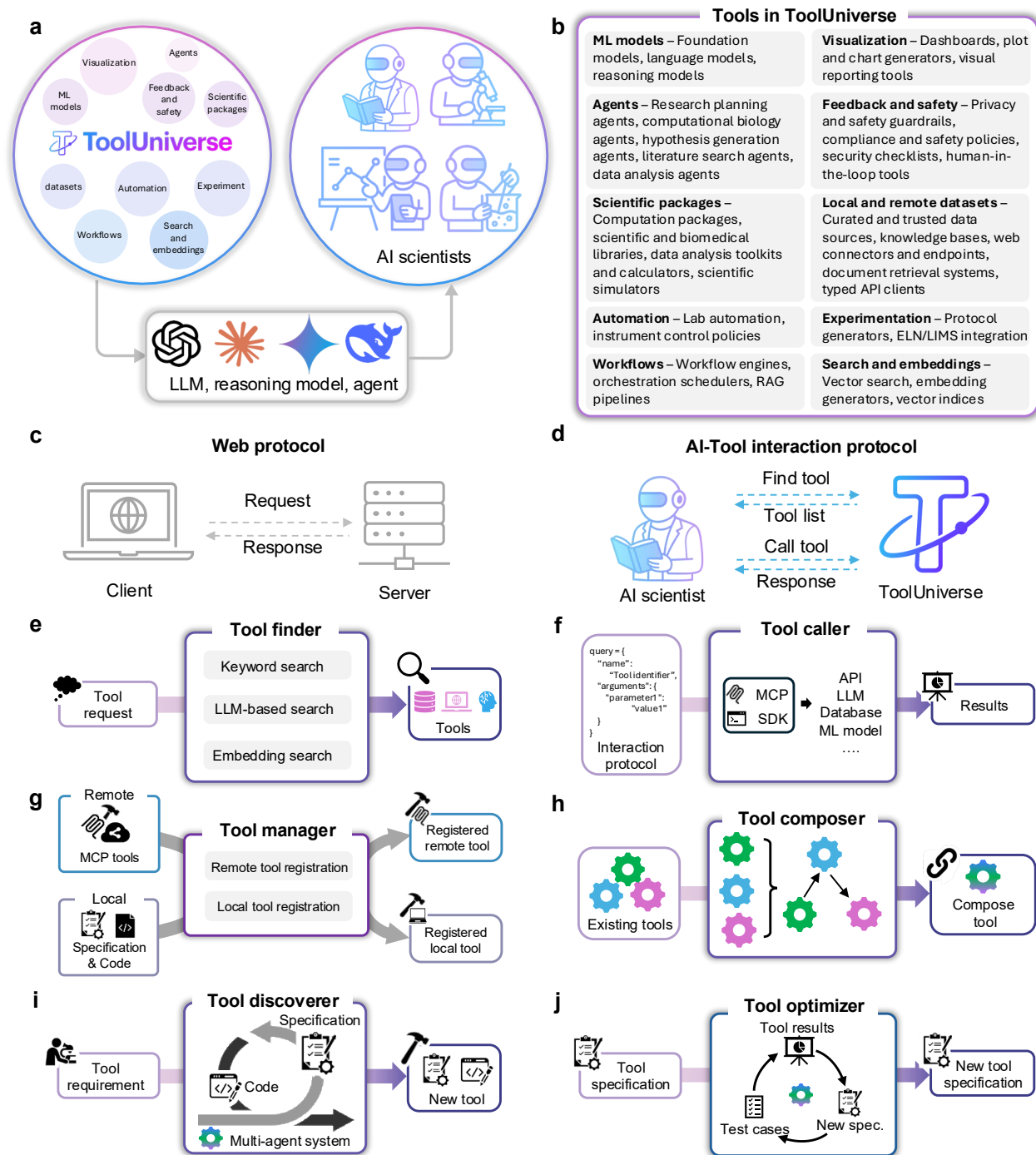


Figure 1

Figure 1: **a)** TOOLUNIVERSE is an ecosystem for building AI scientists. General-purpose LLMs, reasoning models, and agents connect to the TOOLUNIVERSE ecosystem of more than 600 scientific tools to perform autonomous research workflows across domains. Illustrated are four open- and closed-weight AI models: GPT, Claude, Gemini, and DeepSeek. **b)** Overview of the tool categories in TOOLUNIVERSE, including ML models, agents, domain knowledge, experimentation, scientific packages, automation, human feedback, workflows, datasets, APIs, embedding stores, visualization, and retrieval. **c-d)** Like HTTP standardizes client-server communication, TOOLUNIVERSE defines an interaction protocol that governs how AI models issue tool requests and receive responses. Core operations for AI scientists interacting with TOOLUNIVERSE are Find Tool (map natural language to tool specifications) and Call Tool (execute tools and return tool outputs). **e)** Tool Finder identifies relevant tools using keyword search, LLM-based in-context search, and embedding-based similarity search. **f)** Tool Caller validates inputs, dynamically loads tools, dispatches calls through TOOLUNIVERSE.run() or MCP, and returns tool outputs. **g)** Tool Manager integrates local and remote tools. It registers local tools via JSON specifications and decorators and adds remote tools through MCP for privacy- or dependency-constrained setups. **h)** Tool Composer chains multiple tools into composite workflows. It supports sequential, parallel, and feedback-driven orchestration of heterogeneous tools. **i)** Tool Discoverer is a multi-agent system that generates new tools from natural language requirements. It performs specification synthesis, automated code generation, validation, and iterative refinement to produce production-ready tools. **j)** Tool Optimizer is a multi-agent system that iteratively refines tool specifications to improve clarity, accuracy, and usability. It combines test generation, execution analysis, and feedback-driven refinement. ML, Machine Learning; LLM, Large Language Model; HTTP, Hypertext Transfer Protocol; MCP, Model Context Protocol; RAG, Retrieval-Augmented Generation; API, Application Programming Interface; ELN/LIMS, Electronic Lab Notebook and Laboratory Information Management System; SDK, Software Development Kit.

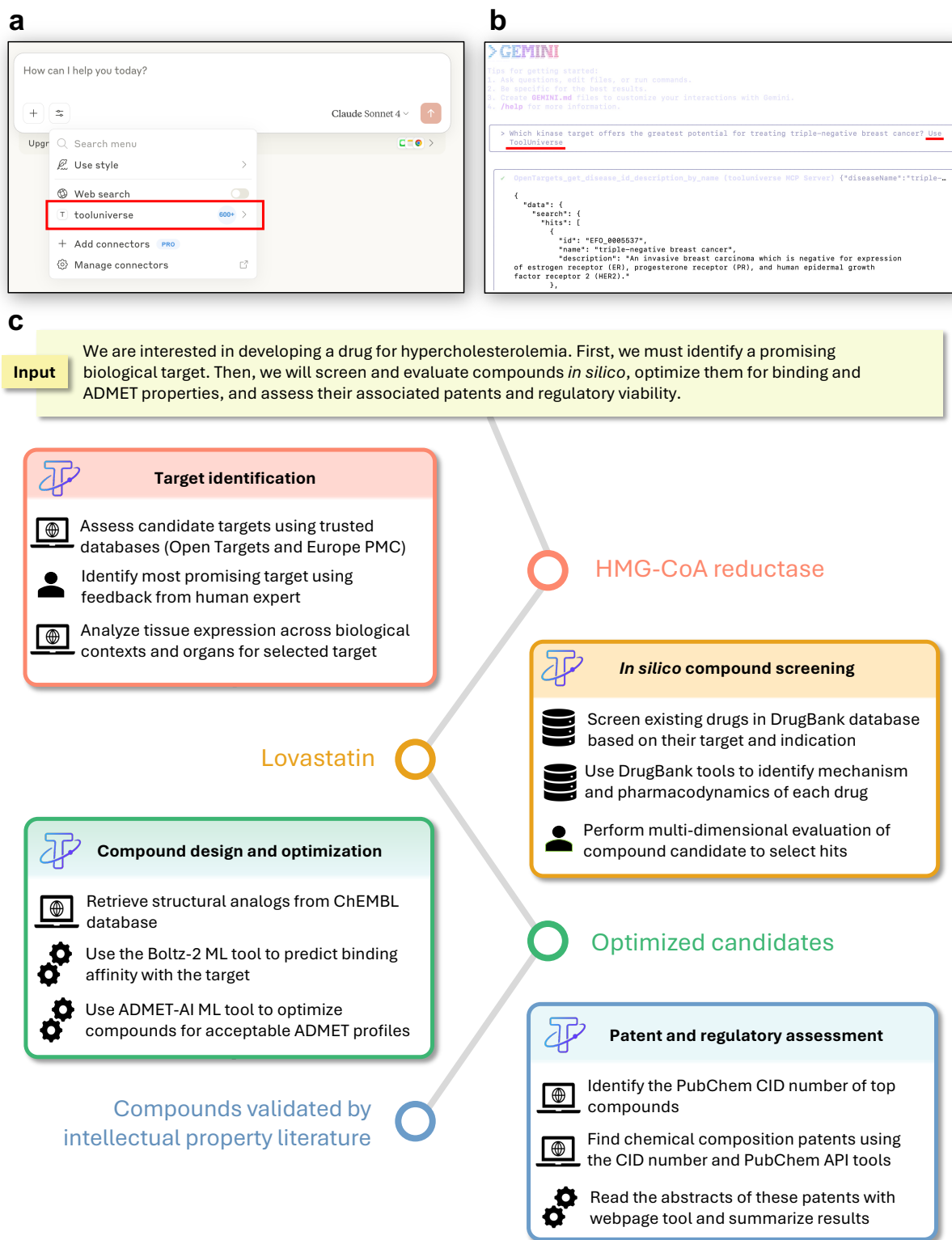


Figure 2

Figure 2: **a)** Building AI scientists by connecting LLMs (for example, Claude) with specialized tools. The AI scientist selects appropriate tools for each task, follows clear instructions, and executes tools from TOOLUNIVERSE. **b)** Building AI scientists with multi-round tool use and reasoning by connecting TOOLUNIVERSE with AI agents (for example, Gemini CLI). These agents identify relevant tools, reason across steps, and iteratively use TOOLUNIVERSE to solve complex, multi-stage scientific problems. **c)** Applying TOOLUNIVERSE to therapeutic discovery for hypercholesterolemia by connecting it with Gemini CLI to create an AI scientist. The analysis proceeds from target identification to compound screening, property optimization, and patent verification. The AI scientist identifies *HMG-CoA reductase* as a therapeutic target, screens existing and novel compounds using DrugBank, ChEMBL, and predictive ML tools such as Boltz-2 and ADMET-AI, and evaluates candidates through patent-mining tools to confirm novelty and prior art. This case study shows how AI scientists chain and execute domain-specific tools, incorporate human feedback, and validate therapeutic hypotheses through multi-step reasoning. Tools from TOOLUNIVERSE used in this illustration of the AI scientist include local datasets (“drugbank get drug name and description by target name”, “drugbank get drug name and description by indication”, “drugbank get pharmacology by drug name or drugbank id”), remote datasets and API tools (“OpenTargets get disease ID description by name”, “OpenTargets get associated targets by disease efoID”, “OpenTargets get target tractability by ensemblID”, “EuropePMC search articles”, “HPA search genes by query”, “HPA get rna expression in specific tissues”, “HPA get comprehensive gene details by ensembl ID”, “ChEMBL search similar molecules”, “PubChem get CID by SMILES”, “PubChem get associated patents by CID”, “get webpage text from URL”), feedback and safety (Consult human expert tool), and ML models (Boltz-2 and ADMET-AI tools). CLI, Command Line Interface; HPA, Human Protein Atlas; ADMET, Absorption, Distribution, Metabolism, Excretion, and Toxicity; CID, Compound Identifier.

Supplementary Information

1 Overview of TOOLUNIVERSE

TOOLUNIVERSE is an ecosystem that wraps around any open or closed AI model, i.e., large language model (LLM), agent, or large reasoning model (LRM), and enables the user to create and refine their own entirely custom AI research assistant (i.e., AI scientist) without the need for additional training or finetuning. To achieve that, TOOLUNIVERSE connects the user-specified LLM/LRM/agent with a scientific toolkit (Supplementary Table 1). While advanced models possess planning and reasoning capabilities, scientific research cannot be conducted through reasoning alone. TOOLUNIVERSE addresses this by providing interactive scientific environments where models can use tools to obtain real-world feedback, effectively transforming internal cognitive processes into tangible research actions. TOOLUNIVERSE features a tool specification protocol that makes tools understandable to LLMs, LRMs, and AI agents regardless of their internal mechanisms, and an interaction protocol that allows tool use without the need to manage backend complexities.

TOOLUNIVERSE is extensible and allows the tools to be easily added, optimized, or created. It hosts a toolkit of over 600 scientific tools. It also supports multi-query specific searches to help users locate relevant tools and is engineered for easy integration with language models, agents, and reasoning models. Current tools in TOOLUNIVERSE include: foundation models, finetuned LLMs, LRMs, and other ML models exposed as callable endpoints; agentic planners and tool routers; domain libraries and simulators; and systems for human-in-the-loop feedback and lab automation with instrument control. TOOLUNIVERSE also provides data and retrieval utilities, such as data sources, knowledge bases, vector search with embedding generators, and complete retrieval-augmented generation (RAG) pipelines. For integration and governance, the ecosystem offers external service connectors, typed API clients, privacy guardrails, safety checklists, compliance controls, and audit logs. TOOLUNIVERSE supports high-level scientific and operational workflows through visualization dashboards, experiment design tools with ELN/LIMS integration, and robust workflow engines and orchestration schedulers. Despite the backend heterogeneity of these tools, which span machine learning models, AI agents, software utilities, robotics, databases, and APIs, all are presented to the AI scientist through a unified AI-interaction protocol, which we describe next.

AI-Tool Interaction Protocol. TOOLUNIVERSE implements a protocol for presenting tool definitions, which makes the backend agnostic to users and simplifies the addition of new tools. This protocol allows the user to equip their AI scientist with tool-use capability without having to handle tool-specific configurations. This protocol has two endpoints: 1) *Find Tool*, which accepts a textual description of a desired functionality and retrieves tools from TOOLUNIVERSE that have the desired functionality, and 2) *Call Tool*, which executes a specified tool with its arguments and returns the results. TOOLUNIVERSE connects to an AI model by providing the definitions of these operations within the model’s context window. This enables the model to leverage its reasoning

capabilities to generate the correct arguments for these operations and to autonomously search for and execute tools.

Core Components. TOOLUNIVERSE include Tool Discoverer and Tool Manager for discovering and integrating tools, a Tool Finder to search for options from over 600 candidates based on user requirements, and a Tool Caller for execution. For complex tasks, the Tool Composer assembles multiple tools into a composite workflow. The Tool Optimizer utilizes a built-in multi-agent system to refine tool specifications, ensuring they better align with the tool’s actual behavior. Leveraging these components and the unified AI-tool interaction protocol, TOOLUNIVERSE empowers creating AI scientists: specialized AI models that combine reasoning with access to curated tools to perform complex research tasks.

2 Unified AI-Tool Interaction Protocol in TOOLUNIVERSE

TOOLUNIVERSE is designed to support a comprehensive ecosystem of tools with exceptionally diverse abilities. Despite the profound backend heterogeneity of these tools, which span machine learning models, AI agents, software utilities, robotics, databases, and APIs, all are presented to the client through a unified protocol.

2.1 Tool Specification Schema

Supplementary Figure 1 shows the tool specification schema in TOOLUNIVERSE. This protocol exposes every tool via a standard specification containing its name; a functional description; a list of parameters, where each parameter is explicitly defined with its own name, description, data type, and required status; and a return schema that shows the data structure of the returned data. An example tool specification is shown in Supplementary Figure 2. The specification is provided to clients such as LLMs, reasoning models, AI agents, and human users to help them understand how to use the tool effectively. For instance, when the client is an LLM, the specification is supplied within its context window, thereby granting it the necessary information to interact with tools from TOOLUNIVERSE.

2.2 AI-Tool Interaction Protocol

TOOLUNIVERSE processes requests through a standard interaction protocol, illustrated in Supplementary Figure 3. All interactions are formatted as a single string that encodes a function call, specifying the desired tool’s name and its input arguments. This protocol provides the foundation for all interactions with TOOLUNIVERSE, enabling a suite of core operations including tool search, calling, discovery, optimization, and composition.

2.3 AI Communication in TOOLUNIVERSE

TOOLUNIVERSE provides two methods for communication: local and remote. For local communication, operations are executed directly in a Python environment using the `TOOLUNIVERSE.run()` function. To support remote serving, TOOLUNIVERSE also implements the Model Context Proto-

Tool Specification Schema in TOOLUNIVERSE

Name: The unique identifier for the tool.

Description: A clear and concise summary of the tool’s purpose and functionality.

Parameters: A list of arguments that the tool accepts. Each argument has the following properties:

- **Argument Name:** The name of the parameter.
- **Argument Type:** The expected data type for the parameter’s value (e.g., string, integer, boolean).
- **Argument Description:** A detailed explanation of what the parameter represents and its purpose.
- **Required:** A boolean value indicating whether the parameter is mandatory for the tool to execute.

Return Schema: A description of the structure and data types of the output returned by the tool upon successful execution.

Supplementary Figure 1: The tool specification schema in TOOLUNIVERSE. The tool specification schema in TOOLUNIVERSE is consistent across all tools, regardless of their diverse backends.

col (MCP), which allows all operations like searching and invoking tools to be communicated with the TOOLUNIVERSE server over a network, eliminating the need for local deployment.

2.4 Accessing Tools from TOOLUNIVERSE

By leveraging a tool specification and interaction protocol, TOOLUNIVERSE provides an interface for human users and AI agents to access tools. The tool can be invoked by executing:

```
tooluniverse.run(tool_call_schema)
```

where `tool_call_schema` is a dictionary following the Interaction Protocol Schema: `{‘name’: name of the tool, ‘arguments’: parameters required by the tool}`. This approach abstracts away backend complexity. Regardless of a tool’s underlying implementation, it is presented to the client (the user of the tool, such as LLMs, reasoning models, AI agents) as a specification. To use a tool, the client consults this specification to construct a request that adheres to the unified AI-tool interaction protocol. This request is then sent to TOOLUNIVERSE via either a local interface or a remote MCP connection. TOOLUNIVERSE processes the request, executes the specified tool, and returns the results to the client. This eliminates the need for complex configurations, regardless

```
[
  {
    "type": "ChEMBLTool",
    "name": "ChEMBL_search_similar_molecules",
    "description": "Search for molecules similar to a given SMILES, chembl_id, or compound or drug name, using the ChEMBL Web Services.",
    "parameter": {
      "type": "object",
      "properties": {
        "query": { "type": "string", "description": "SMILES string, chembl_id, or compound or drug name." },
        "similarity_threshold": { "type": "integer", "description": "Similarity threshold (0-100).", "default": 80 },
        "max_results": { "type": "integer", "description": "Maximum number of results to return.", "default": 20 }
      },
      "required": ["query"]
    }
  }
]
```

Supplementary Figure 2: One example of tool specification in TOOLUNIVERSE.

Interaction schema in TOOLUNIVERSE

Name: The name of the tool or operation to be called.

Parameters: A list of arguments that the tool accepts. Each argument has the following properties:

- **Argument Name:** The name of the parameter.
- **Argument Value:** The value for the parameter provided by the client.

Supplementary Figure 3: The universal interaction schema for all tools and operations within TOOLUNIVERSE.

of backend or runtime differences. For example, users can query a new database without writing database-specific SQL, run machine learning models without configuring GPUs or environments, or access web-based lab equipment through a single, standardized tool call request.

3 Core Components of TOOLUNIVERSE

TOOLUNIVERSE operates through a set of core components designed for comprehensive tool management. Its capabilities include Tool Discoverer to discover new tools and Tool Manager to integrate tools into TOOLUNIVERSE, a Tool Finder to search for suitable options from over 600 candidates based on user requirements, and a Tool Caller for execution. For complex tasks, the Tool Composer assembles multiple tools into a new, composite workflow. The Tool Optimizer utilizes a built-in multi-agent system to refine tool specifications, ensuring they better align with the tool's actual behavior.

3.1 Tool Finder

The TOOLUNIVERSE contains a large repository of scientific tools. To facilitate the creation of a task-specific environment, the tool finder operation is designed to identify and retrieve relevant tools based on user requirements. The input to the tool finder is a natural language query from the client, describing the task they wish to achieve or the specific capabilities required from the tools. It employs a versatile search architecture featuring three distinct methodologies: keyword search, LLM in-context search, and embedding search. The selection of a method allows for a strategic trade-off between search precision, semantic understanding, and computational resource consumption.

Keyword search. Keyword search operates on a sophisticated keyword-based methodology. The process begins by parsing a user’s query through a multi-stage pipeline involving tokenization via regular expressions, the removal of over 45 common English stop words, and suffix-based stemming using 20 morphological rules to reduce words to their root form. To capture multi-word concepts, this method also generates n-grams (bigrams and trigrams). These processed keywords and phrases are then matched against a pre-built index of tool specifications, which has undergone the same processing. Relevance is scored using a term frequency-inverse document frequency (TF-IDF) algorithm, calculated as: $\text{Relevance} = \text{TF} \times \text{IDF} \times \log(1 + \text{QueryFrequency})$, where TF measures how often a term appears in a document, IDF reflects how unique the term is across all documents, and QueryFrequency indicates how often the term appears in the user’s query. The scoring model enhances precision by applying a hierarchical bonus structure to the relevance score. Matches found in a tool’s name receive the highest priority with a 2.0× bonus multiplier, followed by a 1.5× multiplier for exact phrase matches within descriptions. This keyword search approach provides a fast and robust search solution that operates independently of machine learning models, ensuring accessibility across different resource levels.

LLM in-context search. The LLM in-context search leverages the advanced reasoning capabilities of a Large Language Model to interpret user intent more holistically. Rather than relying on simple keyword matching, a detailed prompt for tool selection is constructed. This prompt contextualizes the user’s task description with the tool specifications of a candidate set of tools in TOOLUNIVERSE. The LLM is then tasked with analyzing this rich context to infer the optimal tool or sequence of tools required to fulfill the user’s request. This method excels at interpreting complex, multi-step, or abstract queries that demand logical inference. While its application can be constrained by the finite context window of the model, it offers strong flexibility in understanding abstract goals. The LLM in-context search is powered by the agentic tool implementation in TOOLUNIVERSE. This allows the user to simply provide a configuration file that defines the prompt and tool specifications, without needing to manage the backend LLM inference processes.

Embedding search. Embedding search is a highly scalable method that retrieves tools by matching the semantic similarity between a user’s query and the tool’s description. To achieve this, we finetune the GTE-Qwen2-1.5B language embedding model using pairs of synthetic user queries

```

def run(self, arguments):
    query = arguments.get("query")
    similarity_threshold = arguments.get("similarity_threshold", 80)
    max_results = arguments.get("max_results", 20)

    if not query:
        return {"error": "`query` parameter is required."}
    return self._search_similar_molecules(query, similarity_threshold, max_results)

```

Supplementary Figure 4: Code example of a tool operation implementation used by the Tool Caller during execution.

and augmented tool specifications, training it to understand the connection between a user’s intent and a tool’s function. The process involves two stages. First, in an offline indexing stage, each tool’s specification is passed through the embedding model to generate a semantic vector that captures its meaning. These vectors are then stored and indexed in a specialized vector database. Later, during the online querying stage, a user’s natural language query is converted into a query vector using the same model. Finally, relevant tools are discovered by calculating the cosine similarity between the user’s query vector and all the tool vectors in the database, identifying the closest matches.

3.2 Tool Caller

The Tool Caller is the primary execution engine in TOOLUNIVERSE. It is responsible for instantiating tools, validating requests, and dispatching calls. Upon initialization, the Tool Caller is configured with a manifest of available tools, including their specifications and settings. To mitigate the significant system overhead associated with loading all tools simultaneously, it employs a dynamic loading strategy. A specific tool is loaded into memory only upon its first request and is then cached for a duration to efficiently handle subsequent calls. During this loading process, the Tool Caller injects the necessary configurations, such as API endpoints and authentication keys, into the corresponding tool class.

When a tool execution request is received, the Tool Caller first parses it to extract the tool name and arguments. It then performs a rigorous validation check, ensuring the provided arguments conform to the data types and structural requirements defined in the tool’s specification. Once validated, the Tool Caller dispatches the arguments to the tool’s primary execution method, such as `run()`, as illustrated in Supplementary Figure 4. The resulting output is then returned to the client through the TOOLUNIVERSE’s communication protocols. If any step in this process fails, from loading to validation or execution, the system generates and returns a descriptive error message. This feedback mechanism helps the client diagnose the issue and revise the request accordingly.

```

from tooluniverse.tool_registry import register_tool

@register_tool('MyTool', config={
    "name": "my_tool",
    "type": "MyTool",
    "description": "Does something useful",
    "parameter": {
        "type": "object",
        "properties": {
            "input": {"type": "string", "description": "Your input"}
        },
        "required": ["input"]
    }
})

class MyTool:
    def __init__(self, tool_config=None):
        self.tool_config = tool_config

    def run(self, arguments):
        return {"result": f"Processed: {arguments['input']}", "success": True}

```

Supplementary Figure 5: Example code demonstrating how to register a local tool with Tool Manager and add it to TOOLUNIVERSE.

3.3 Tool Manager

Tool Manager is designed to simplify the process of adding new tools to TOOLUNIVERSE. Tool Manager simplifies the addition of new tools through two modes: local tools and remote tool integration. For local tools, which require no special dependencies, only a JSON specification (including name, descriptions, arguments, and configurations) and a corresponding function are needed. The function executes the tool call arguments. For remote tools, which may have special dependencies or cannot be open-sourced, TOOLUNIVERSE offers a wrapper that links them as external tools via the MCP.

Local Tool Registration. For local tool registration, to add a tool to TOOLUNIVERSE, both a tool configuration and a corresponding tool class are required. The tool configuration is a dictionary that specifies the tool according to the Tool Specification Schema of TOOLUNIVERSE and includes the necessary settings for its execution. The tool class defines an initialization function that sets up the tool based on its specification, as well as a run function that processes tool call arguments in accordance with the Interaction Protocol Schema of TOOLUNIVERSE. Local tool registration within the Tool Manager is facilitated through an easy-to-use decorator function, `register_tool(Class_name, tool_config)`, which decorates the tool class as illustrated in Supplementary Figure 5. Here, `Class_name` is the string name of the tool class, and

```

from tooluniverse.mcp_tool_registry import register_mcp_tool, start_mcp_server

@register_mcp_tool(
    tool_type_name="my_analyzer",
    config={
        "description": "Analyzes data and returns results",
        "parameter_schema": {
            "type": "object",
            "properties": {
                "data": {"type": "string", "description": "Data to analyze"}
            },
            "required": ["data"]
        }
    },
    mcp_config={
        "server_name": "My Analysis Server",
        "port": 8001,
        "host": "0.0.0.0"
    }
)

class MyAnalyzer:
    def run(self, arguments):
        data = arguments.get('data', '')
        return {"result": f"Analyzed: {data}", "success": True}

```

Supplementary Figure 6: Example code demonstrating how to register a remote tool with Tool Manager and add it to TOOLUNIVERSE.

`tool_config` is the configuration containing both the tool specification and required settings. Once registered, the tool is automatically integrated into TOOLUNIVERSE without further manual configuration. This registration process allows users to incorporate custom tools into TOOLUNIVERSE. This enables coordination with other existing tools, thereby empowering the creation of customized AI scientists.

Remote Tool Registration. Remote Tool Registration enables the integration of tools that are private, require specialized configurations, or operate within restricted environments, and therefore cannot be made publicly available. Once registered remotely, these tools are added to TOOLUNIVERSE and can be accessed and executed in the same manner as standard tools.

To achieve this, the Tool Manager includes an automatic MCP Auto Loader Tool that accepts the address of an MCP server and registers all of its tools into the TOOLUNIVERSE's tool list. After the MCP Auto Loader Tool has loaded the remote tools, they are integrated into the TOOLUNIVERSE with the same functionality as other tools. For the remote side, TOOLUNIVERSE supports two methods for setting up a remote tool. The first is building standard tools that support MCP. To

further simplify the process and make remote tool registration identical to local registration, the Tool Manager also provides a decorator function, `register_remote_tool(Class_name, tool_config, mcp_config)`. In this function, the `Class_name` and `tool_config` parameters are the same as those used in `register_tool(Class_name, tool_config)`, while `mcp_config` defines the configuration for the MCP server, such as the host address and port used for the service.

```
def compose(arguments, tooluniverse, call_tool):
    """Search literature and generate summary"""
    topic = arguments['research_topic']

    literature = {}
    literature['pmc'] = call_tool('EuropePMC_search_articles', {'query': topic, 'limit': 5})
    literature['openalex'] = call_tool('openalex_literature_search', {'search_keywords': topic, 'max_results': 5})
    literature['pubtator'] = call_tool('PubTator3_LiteratureSearch', {'text': topic, 'page_size': 5})

    summary = call_tool('MedicalLiteratureReviewer', {
        'research_topic': topic, 'literature_content': str(literature),
        'focus_area': 'key findings', 'study_types': 'all studies',
        'quality_level': 'all evidence', 'review_scope': 'rapid review'
    })

    return summary
```

Supplementary Figure 7: This example demonstrates a composable tool, built with the Tool Composer, that runs multiple literature search tools concurrently, followed by a summary agent that synthesizes the results. The Tool Composer enables the combination of multiple tools from TOOLUNIVERSE in diverse ways, such as in parallel, sequentially, or in loops, enabling multi-tool collaboration.

3.4 Tool Composer

For complex tasks, users can create new composite tools by programmatically combining existing ones. Tool Composer enables the integration of tools with heterogeneous back ends to build end-to-end workflows. Leveraging the Tool Caller for direct in-code execution, Tool Composer generates a container function that exposes both the Tool Caller and TOOLUNIVERSE as in-line, executable primitives. The container function, implemented as `compose(arguments, tooluniverse, call_tool)`, serves as the execution backbone for Tool Composer. It contains the logic for coordinating different types of tools so they work together in a single workflow. The `arguments` parameter specifies the tool call arguments that follow the interaction protocol schema of TOOLUNIVERSE, the `tooluniverse` is an instance of TOOLUNIVERSE that provides all available functions that TOOLUNIVERSE can support, and the `call_tool` parameter is a callable interface of Tool Caller that abstracts the invocation of individual tools in TOOLUNIVERSE. By integrating these components, the container function enables flexible multi-tool execution patterns, such as chaining outputs between tools, broadcasting a single query across multiple tools, and constructing agentic loops that leverage tool feedback for adaptive, multi-step

experimental analysis. It can chain the output of one tool into the input of the next, call multiple tools with a single query, and build agentic loops that use an agentic tool to generate function calls, execute tools, and incorporate tool feedback for multi-step experimental analysis. As illustrated in Supplementary Figure 7, a composed tool can run several literature search tools concurrently and then invoke a summarization agent to synthesize the findings, demonstrating heterogeneous workflow construction in which each step is driven by tool execution.

3.5 Tool Optimizer

Tool Optimizer is designed to refine a tool’s specifications, ensuring they are clear, accurate, and easily understood by models. Taking advantage of the workflow building of TOOLUNIVERSE using Tool Composer, we build an agentic tool description optimization tool, where the tool description is optimized by an iterative multi-round process that combines automated test case generation, real tool execution analysis, and agentic-powered feedback refinement. Through feedback-driven iterations, the system progressively improves both tool descriptions and parameter specifications, eliminating redundancy between them while ensuring accuracy through empirical validation. The optimization process automatically terminates when quality thresholds are met or maximum iterations are reached, producing specifications that enhances tool usability for AI agents.

Core principles and tools. We develop the Tool Optimizer that employs a multi-round iterative optimization strategy to automatically enhance tool documentation quality. The optimizer is built on three core principles: (1) test-driven optimization that validates descriptions against actual tool execution results, (2) multi-dimensional quality assessment across six standardized criteria, and (3) feedback-driven improvement that leverages insights from previous optimization rounds to guide subsequent iterations. The optimizer implements a compositional architecture consisting of four specialized components working in concert. The TestCaseGenerator creates diverse test scenarios based on tool configurations and adaptively generates targeted test cases in later rounds using feedback from previous iterations. The DescriptionAnalyzer examines the alignment between existing descriptions and actual tool behavior by analyzing test execution results, then generates optimized descriptions that better reflect the tool’s true functionality. The ArgumentDescriptionOptimizer specifically targets parameter descriptions to ensure consistency with real usage patterns while eliminating redundancy between tool and parameter documentation. Finally, the DescriptionQualityEvaluator provides objective scoring on a 0-10 scale across six quality dimensions: clarity, accuracy, completeness, conciseness, user-friendliness, and redundancy avoidance.

Optimization process. The optimization process begins with initial test case generation followed by tool execution to gather baseline performance data. The system then enters an iterative optimization loop where each round generates enhanced test cases based on previous feedback, analyzes accumulated test results to propose improved descriptions, optimizes both tool and parameter descriptions, and evaluates quality against predefined thresholds. The process continues until either the satisfaction threshold is met (typically 8.0/10 for production use) or the maximum iteration

limit is reached (default: 3 rounds). This adaptive approach ensures comprehensive coverage while maintaining computational efficiency.

3.6 Tool Discoverer

Tool Discoverer automatically generates new tools, including both specifications and executable code, from high-level natural language descriptions. Leveraging the workflow composition capabilities of TOOLUNIVERSE via Tool Composer, we construct an agentic multi-stage pipeline that transforms a plain-text functional request into a production-ready tool with minimal human intervention. The process integrates tool discovery, structured specification generation, code implementation, and iterative quality refinement, ensuring that the final tool adheres to functional requirements and ecosystem conventions.

Through iterative feedback loops combining search, analysis, and code optimization, the system progressively improves the generated tool until it reaches predefined quality standards. The process terminates when target scores are achieved or iteration limits are reached, producing tools that are robust, maintainable, and ready for deployment.

Core principles and architecture. The Tool Discoverer system is built around four core principles: pattern-guided generation that reuses functional patterns and conventions from existing tools to ensure ecosystem consistency; structured specification synthesis that transforms unstructured requests into tool specifications; automated code generation and validation that produces executable implementations with integrated testing; and iterative refinement that uses feedback from analysis and testing to drive targeted improvements.

The system integrates four specialized components. The tool finder locates existing tools with similar functionality using semantic similarity and keyword-based search, ensuring adherence to established conventions. The SpecificationGenerator converts the natural language description into a structured specification, including tool name, description, parameter definitions, return schema, and category metadata. The ImplementationGenerator produces code that follows best practices, includes complete dependency handling, integrates with the TOOLUNIVERSE registry, and implements error handling for robust operation. The QualityEvaluator assesses the generated tool across functionality, reliability, maintainability, performance, and test coverage, scoring each dimension from 0–10 and computing an overall weighted score.

Generation process. The generation workflow begins with the discovery stage, which accepts a tool description as inputs. It applies multiple search strategies to retrieve similar tools. Results are validated, deduplicated, and compiled into a final set of references. Next, the specification stage uses an agentic tool to produce a complete tool configuration. This includes tool name, descriptions, parameter definitions with type annotations and descriptions, JSON-schema-based return type specification, and other meta data. The output conforms to TOOLUNIVERSE schema requirements and naming conventions, enabling immediate downstream integration. The implementation phase employs template-driven code generation to produce production-ready code, incorporating

required imports, type-hinted function signatures, error handling, integration hooks via the `@register_tool` decorator in `TOOLUNIVERSE`, and a deployment-ready module structure. Finally, the system conducts a multiple quality assessments, combining code analysis, dynamic testing with auto-generated test cases, and performance profiling. Each dimension is scored, with a target minimum of 9/10 for production deployment. An iterative refinement loop applies targeted improvements until the threshold is met. Generated tools are packaged for immediate inclusion in `TOOLUNIVERSE`, producing a JSON configuration file with metadata, a source file with the complete implementation, and dependency specifications for reproducible installation.

4 Building AI scientists with TOOLUNIVERSE

A customized AI scientist can be developed by integrating `TOOLUNIVERSE` with LLMs, reasoning models, and AI agents. In this configuration, the LLMs and reasoning models provide the core capabilities for reasoning and tool usage, while `TOOLUNIVERSE` serves as the scientific environment for interaction and experimentation. The development process typically involves three steps: 1) installing `TOOLUNIVERSE` with a single command (`pip install tooluniverse`); 2) connecting `TOOLUNIVERSE` to the chosen model so it can access the tools provided by `TOOLUNIVERSE`; and 3) instructing the model to use these tools to address a given scientific problem.

Once the setup is complete, the AI scientist operates as follows: given a user instruction or task, it formulates a plan or hypothesis, employs the tool finder in `TOOLUNIVERSE` to identify relevant tools, and iteratively applies these tools to gather information, conduct experiments, verify hypotheses, and request human feedback when necessary. For each required tool call, the AI scientist generates arguments that conform to the `TOOLUNIVERSE` protocol, after which `TOOLUNIVERSE` executes the tool and returns the results for further reasoning.

The models used to construct AI scientists can include LLMs, reasoning models, and AI agents. LLMs may be API-based, such as GPT, Claude, or Gemini, or open-weight models, such as LLaMA, DeepSeek, or Qwen. Large reasoning models enhance problem-solving capabilities by applying built-in chains of thought to analyze the current step before interacting with `TOOLUNIVERSE`. Agentic systems, such as Gemini CLI or Claude Code, integrate reasoning models with agentic feedback loops to autonomously manage multi-step problem solving and tool use. In addition to general-purpose agents, `TOOLUNIVERSE` can be paired with specialized agents trained for specific scientific domains, enabling stronger performance on targeted tasks. The following sections present three examples of building AI scientists using LLMs, agentic systems, and specialized agents.

4.1 Building an AI Scientist from an LLM or an LRM

Figure 2b illustrates an example of building an AI scientist using an LLM, such as Claude, together with `TOOLUNIVERSE`. The process involves only three steps.

1. Install `TOOLUNIVERSE` with a single command and install the Claude desktop app.

2. Open the Claude Desktop and navigate to Settings → Developer → Edit Config. Set up the configurations as follows:

```
{
  "mcpServers": {
    "tooluniverse": {
      "command": "uv",
      "args": [
        "--directory",
        "path_to_ToolUniverse/src/tooluniverse",
        "run",
        "tooluniverse-mcp-claude"
      ]
    }
  }
}
```

3. Launch the Claude Desktop, select tools in TOOLUNIVERSE for the desired tasks.

4.2 Building an AI Scientist from an AI Agent

We demonstrate how to build an AI scientist using AI Agents, such as the Gemini CLI, together with TOOLUNIVERSE. While AI Agents can automatically leverage TOOLUNIVERSE's tool finder to identify the tools required for specific tasks, the process of creating an AI scientist involves just two steps.

1. Install TOOLUNIVERSE with a single command and install the Gemini CLI.
2. Open the setting configuration file for Gemini CLI. Set up the configurations as follows:

```
{
  "mcpServers": {
    "tooluniverse": {
      "command": "uv",
      "args": [
        "--directory",
        "/path/to/your/gemini_running_env",
        "run",
        "tooluniverse-smcp-stdio"
      ]
    }
  },
}
```

4.3 Building an AI Scientist from a Specialized AI Agent

Specialized AI agents are trained on specific types of tasks, allowing them to become experts in particular domains, such as the TxAgent [13] for precision therapeutics, GeneAgent [16] for gene-set analysis, and SpatialAgent [39] for spatial biology. In TxAgent [13], TOOLUNIVERSE can be used not only by these specialized AI agents during inference but also as a real-world environment for agent training. In training, TOOLUNIVERSE serves as the scientific environment in which TxAgent can interact. Through reinforcement learning, TxAgent learns how to use tools within TOOLUNIVERSE and effectively manage complex therapeutic tasks.

Tool category	Description
ML models	Tools that apply machine learning algorithms to tasks like prediction, classification, or generation. Examples include foundation models, language models, and reasoning models.
Agents	Tools that operate autonomously to perceive environments, make decisions, and take actions toward goals. Examples include research planning agents, hypothesis generation agents, and data analysis agents.
Scientific packages	Software packages engineered to facilitate diverse scientific tasks, experiments, and data analysis workflows. Examples include computation packages, biomedical libraries, and scientific simulators.
Automation	Tools involving physical or simulated machines capable of sensing, reasoning, and acting in the world. Examples include lab automation tools and instrument control policies.
Workflows	Tools that enable complex, multi-step scientific workflows. Examples include orchestration schedulers and RAG pipelines.
Visualization	Tools that facilitate the display and communication of scientific data and results. Examples include dashboards and plot and chart generators.
Feedback and safety	Tools that incorporate evaluations or input from human experts to ensure safety and goal alignment. Examples include privacy guardrails, security checklists, and human-in-the-loop tools.
Local and remote datasets	Tools that store, manage, and query structured or semi-structured data efficiently, including relational, tabular, and hierarchical datasets. Examples include knowledge bases and typed API clients.
Experimentation	Tools that support the design and management of experiments. Examples include protocol generators and LIMS integration tools.

Search and embeddings	Tools that store and retrieve vectorized representations of data for use in machine learning tasks. Examples include vector search tools and embedding generators.
-----------------------	--

Supplementary Table 1: Types of tools in TOOLUNIVERSE that TOOLUNIVERSE-powered AI scientists can use.

Tool category	Number	Examples of tools in TOOLUNIVERSE
ML models	17	boltz2_docking, run_TxAgent_biomedical_reasoning, ADMET_predict_CYP_interactions
Agents	56	HypothesisGenerator, CodeQualityAnalyzer, MedicalLiteratureReviewer
Scientific packages	164	get_biopython_info, get_pyscreener_info, get_pykalman_info
Automation	8	communicate_with_ros_robot, mcp_auto_loader, mcp_client
Workflows	11	biomarker_discovery_workflow tool_optimizer tool_discoverer
Visualization	3	visualize_protein_structure_3d visualize_molecule_2d visualize_molecule_3d
Feedback and safety	6	consult_human_expert, get_expert_response, get_expert_status
Local and remote datasets	391	drugbank_get_drug_pathways_and_reactions_by_name, HPA_get_comprehensive_gene_details_by_ensembl_id, FDA_get_active_ingredient_info_by_drug_name, OpenTargets_get_associated_targets_by_disease_efoId

Search and embeddings	4	embedding_tool_finder, embedding_database_search, embedding_database_add
Experimentation	3	experimental_design_scorer, protocol_optimizer, extract_clinical_trial_outcomes

Supplementary Table 2: Number of tools and example tools for each category in TOOLUNIVERSE. The table shows the number of tools as of October 11, 2025. Note that TOOLUNIVERSE is continually expanded with new tools.

5 Tools in TOOLUNIVERSE

TOOLUNIVERSE is a scientific environment that contains over 600 tools covering essential scientific research domains. TOOLUNIVERSE integrates built-in tool categories that are easy for people to reuse, covering machine learning models, AI agents, software utilities, expert feedback systems, robotics, databases, embedding stores, data archives, and APIs, each serving specific computational and analytical requirements.

Agentic tools. Agentic tools operate autonomously to perform complex tasks using LLMs. Each agent is configurable with custom prompts and tool specifications, supporting multiple backend models, including ChatGPT and Gemini. TOOLUNIVERSE includes agentic tools for literature summarization, code analysis, hypothesis generation, experiment planning, and results analysis. By defining the prompts and tool specifications in the configuration file, one can quickly build an agentic tool.

Scientific software package tools. To support scientific coding, scientific package tools provide comprehensive information about Python-based scientific computing libraries such as NumPy, Pandas, and SciPy. These tools offer installation instructions, usage examples, and documentation links, implementing dual-source data retrieval from PyPI APIs with local backup information.

Database tools. Database tools manage structured scientific resources such as DrugBank vocabulary datasets, clinical trial records, and molecular databases. They support integrations with tabular, hierarchical, XML-based, and graph-structured data. These tools provide capabilities for text-based search, field-level filtering, configurable result limits, and metadata return schemas. Built-in search, filtering, and indexing features can be reused when incorporating new databases.

API integration tools. API integration tools enable communication with external scientific data sources using standard protocols such as RESTful APIs or GraphQL. Through these tools, users can access resources like FDA drug databases, OpenTargets disease–target associations, PubChem compound information, and many other databases, all with robust error handling and response validation. New tools can be incorporated by updating the API server URL, provided the common protocol is maintained.

Expert feedback tools. Expert feedback tools integrate human expertise directly into the environ-

ment, allowing AI scientists to request human suggestions or approval whenever necessary. This tool includes a server that connects the system with human experts, along with a user interface through which experts can provide responses. When a user calls the expert feedback tool, the request is redirected by the tool caller in TOOLUNIVERSE to a server, which forwards it to the human expert interface. Human experts can receive the request and provide their own insights and judgments. Their feedback is then sent back through the server as a tool response to the user. This approach enables consultation with human experts for complex scientific decisions and interpretations, effectively combining automated analysis with expert validation.

Machine learning tools. Machine learning tools apply predictive and generative models to scientific use cases, such as disease–target scoring [40], disease-state prediction, gene-gene interaction [41, 42], gene dependency analysis [43], ADMET prediction [25], binding affinity prediction [24], and beyond. Since running environments for machine learning models often require specialized setups and hardware (e.g., GPUs), which can be difficult to deploy, TOOLUNIVERSE uses a remote registration scheme. This approach allows models to run on private servers while still being exposed as tools within TOOLUNIVERSE. New machine learning models can be quickly integrated into TOOLUNIVERSE through remote tool registration.

Embedding store tools. Embedding store tools manage vectorized representations of scientific data. Scientific data is first transformed into embeddings using embedding models and then stored in a database. TOOLUNIVERSE employs FAISS to enable efficient semantic search, similarity matching, and data retrieval over these embedding databases.

6 Evaluation of Tools

To ensure the correctness and reliability of tools before their inclusion in TOOLUNIVERSE, we implemented a multi-step evaluation process. This evaluation was designed both to validate tool functionality and to ensure scientific utility. The evaluation steps are as follows:

- **Input-output sampling.** For each tool, we generated diverse sample inputs and recorded corresponding outputs. These samples were constructed to cover typical use cases as well as edge conditions, ensuring broad coverage of tool functionality.
- **Human-in-the-loop review.** Outputs produced by the tools were subjected to systematic human review. Scientific experts assessed correctness, interpretability, and consistency with expected domain knowledge. This human evaluation provided an additional safeguard against erroneous or misleading outputs.
- **Automated optimizers and checkers.** Complementing human evaluation, we employed automated optimizer and checker tools. These systems iteratively tested tool specifications against the sampled inputs, refining descriptions and ensuring consistency between declared functionality and observed behavior. This process emphasized correctness and usability, rather than accuracy alone, to promote robust integration within the ecosystem.

- **Regular maintenance and bug reporting.** For continued reliability of tools within TOOLUNIVERSE, we perform regular maintenance and monitoring. A structured bug reporting system allows issues to be identified by users and promptly addressed by the TOOLUNIVERSE team. These practices provide ongoing quality assurance and safeguard the long-term usability of the ecosystem.

Beyond these processes, TOOLUNIVERSE prioritizes tools from trusted sources. Many included tools have been published, peer-reviewed, and verified through prior use by established scientific communities, such as the NIH, FDA, and other regulatory or research agencies. By relying on previously validated resources, we reduce the risk of introducing spurious or unverified functionality into the ecosystem. These evaluation measures ensure that tools incorporated into TOOLUNIVERSE meet standards of correctness, reproducibility, and scientific reliability, providing a foundation for dependable AI-assisted discovery.

7 Further Details on the Case Study of TOOLUNIVERSE

We provide details for the hypercholesterolemia use case shown in Figure 2c, where an AI scientist powered by LLMs connected to TOOLUNIVERSE finds and optimizes statin compounds for hypercholesterolemia. Through this case study, we show how TOOLUNIVERSE can be used for highly interdisciplinary and complex scientific methods like drug development. We demonstrate that a TOOLUNIVERSE-enabled AI scientist is able to recover existing research on statins, lending credibility to the research enabled by TOOLUNIVERSE.

The AI scientist is constructed by providing all 600+ tools in TOOLUNIVERSE to Gemini CLI (powered by the Gemini-2.5-Pro model). With this current AI scientist, we must prompt the model with high-level prompts to achieve each stage of the case study. We envision that future TOOLUNIVERSE-enabled AI scientists will be knowledgeable enough about TOOLUNIVERSE and the scientific discovery process to require only a single high-level prompt and occasional expert feedback to achieve the entire case study.

In our case study, the AI scientist is first prompted to conduct target identification for hypercholesterolemia. The AI scientist first calls `OpenTargets.get_disease_id_description_by_name` (API Tool) and `OpenTargets.get_associated_targets_by_disease_efo_id` (API Tool), which allow it to identify the top targets associated with the disease. Next, it calls `OpenTargets.get_target_tractability_by_ensemblID` (API Tool) and `EuropePMC.search_articles` (API Tool) on each protein target. These tools provide diverse information about each protein’s potential as a target, including the existence of approved drugs for the target, the presence of a high-quality binding pocket, and associated literature. After retrieving this information for each target, the AI scientist calls `consult_human_expert` (Expert Feedback Tool) to perform scientist-guided selection of the final target based on the existing literature. In this way, the AI scientist identifies eleven protein targets involved in hypercholesterolemia, conducts extensive literature reviews on each, and selects HMG-CoA reductase as the target to take forward due

to its history of successful targeting with statins. Next, the AI scientist uses `HPA_search_genes_by_query` (API Tool), `HPA_get_rna_expression_in_specific_tissues` (API Tool), and `HPA_get_comprehensive_gene_details_by_ensembl_id` (API Tool) to query the Human Protein Atlas and characterize the expression profile of HMG-CoA reductase. Using the atlas data, the AI scientist concluded that there is high expression in the liver (the tissue of interest), but also in locations such as the gastrointestinal tract and brain. It reasoned that this could explain certain off-target effects associated with targeting HMG-CoA reductase, such as neurological side effects. Thus, minimizing off-target binding and side effects is crucial to consider in subsequent screening steps.

The AI scientist now conducts an *in silico* screen and molecular optimization process. It first calls `drugbank_get_drug_name_and_description_by_target_name` (Database Tool) and `drugbank_get_drug_name_and_description_by_indication` (Database Tool) to retrieve current statin treatments from the DrugBank database, as statins target HMG-CoA reductase. The AI scientist then profiles each statin with `drugbank_get_pharmacology_by_drug_name_or_drugbank_id` (Database Tool). This result in the selection of lovastatin as the statin to optimize. Lovastatin is a widely used medication but has off-target binding in non-liver tissues compared to hydrophilic statins. To optimize lovastatin, the AI scientist uses `ChEMBL_search_similar_molecules` (API Tool) to retrieve molecular candidates from the ChEMBL database that are structural analogs to lovastatin (Tanimoto similarity > 0.80). Then, two TOOLUNIVERSE ML Model Tools (`ADMETAI_predict_admet_properties` and `boltz2_docking`) are used to retrieve key pharmaceutical properties for each of the 32 structural analogs, including ADMET properties and binding affinity to HMG-CoA reductase. Of note, though Boltz-2 has strong performance on binding likelihood and affinity predictions, there is variability in the model output given the same input, so Boltz-2 was run four times for each of the structural analog candidates, and the mean and standard deviation of its outputs were calculated. Predictions from the ML Model Tools for select properties are shown in Supplementary Table 3. We focus particularly on binding likelihood, binding affinity, and probability of blood-brain-barrier (BBB) penetrance because the former two assess the molecule’s ability to act on its target, HMG-CoA reductase, while the latter assesses the molecule’s probability of penetrating into one of the tissues where its target is highly expressed (brain), which could lead to off-target effects.

ChEMBL ID	Preferred name	Prob. of binding mean (↓)	Prob. of binding std. dev.	Binding affinity mean	Binding affinity std. dev.	Prob. of BBB penetrance
CHEMBL3349960		0.48	0.08	0.54	0.41	0.58
CHEMBL2347006		0.44	0.09	-0.18	0.13	0.48
CHEMBL1205793		0.43	0.04	0.38	0.30	0.68

ChEMBL ID	Preferred name	Prob. of binding mean (↓)	Prob. of binding std. dev.	Binding affinity mean	Binding affinity std. dev.	Prob. of BBB pene-trance
CHEMBL1515625		0.41	0.10	0.59	0.12	0.59
CHEMBL3970138		0.41	0.10	-0.09	0.33	0.47
CHEMBL1394089		0.40	0.10	0.54	0.38	0.62
CHEMBL3186637		0.40	0.05	0.02	0.11	0.73
CHEMBL152032	mevinolin	0.39	0.06	0.04	0.16	0.69
CHEMBL1207599		0.38	0.05	0.28	0.40	0.55
CHEMBL1230589		0.38	0.06	0.71	0.03	0.64
CHEMBL3349881		0.38	0.07	0.45	0.12	0.57
CHEMBL4088701		0.37	0.04	0.24	0.20	0.60
CHEMBL333443		0.37	0.08	0.60	0.26	0.58
CHEMBL303515	lovastatin sodium	0.34	0.02	0.25	0.22	0.56
CHEMBL2364554		0.34	0.05	0.48	0.13	0.49
CHEMBL175236		0.34	0.06	0.15	0.24	0.54
CHEMBL330439		0.34	0.11	0.54	0.40	0.58
CHEMBL1206749		0.34	0.05	0.20	0.24	0.59
CHEMBL1456346		0.33	0.09	0.40	0.37	0.55
CHEMBL418776		0.33	0.06	0.16	0.07	0.52
CHEMBL1201373	lovastatin acid	0.31	0.08	0.16	0.12	0.57
CHEMBL487721		0.31	0.07	0.19	0.14	0.54
CHEMBL1317360		0.29	0.15	0.46	0.24	0.51
CHEMBL5281241		0.29	0.14	0.44	0.31	0.47
CHEMBL3544685		0.27	0.04	0.37	0.18	0.50
CHEMBL4076715		0.25	0.10	0.16	0.21	0.44
CHEMBL1144	pravastatin	0.24	0.12	0.44	0.26	0.48
CHEMBL3544686		0.23	0.04	0.72	0.28	0.54
CHEMBL3187243		0.22	0.04	0.44	0.11	0.64
CHEMBL690	pravastatin sodium	0.22	0.02	0.55	0.08	0.43
CHEMBL3544781		0.22	0.03	0.24	0.28	0.50
CHEMBL1617336		0.21	0.04	0.32	0.13	0.57

ChEMBL ID	Preferred name	Prob. of binding mean (↓)	Prob. of binding std. dev.	Binding affinity mean	Binding affinity std. dev.	Prob. of BBB pene- trance
-----------	----------------	------------------------------	----------------------------	-----------------------	----------------------------	------------------------------

Supplementary Table 3: TOOLUNIVERSE output for all 34 structural analogs of lovastatin. Binding probability and affinity were predicted by Boltz-2, while the probability of blood-brain-barrier (BBB) penetrance was predicted by ADMET AI. For binding affinity, more negative values indicate higher binding affinity. Analogs are ranked in descending order by predicted probability of binding. Mean and standard deviation were calculated across four samples. The two rows highlighted in red indicate the small molecule candidate (CHEM-BL2347006/CHEMBL3970138) that is selected for additional downstream evaluation in the patent literature.

The FDA-approved pravastatin and its charged form, pravastatin sodium, appear in the list of structural analogs and, based on the ML model outputs, have lower probability of BBB penetrance compared to lovastatin. This is consistent with pravastatin’s lower off-target binding outside the liver, thus supporting the AI scientist’s TOOLUNIVERSE-based optimization protocol for addressing the weaknesses in lovastatin with new therapeutic candidates.

Finally, we use the AI scientist’s outputs to select two structural analogs for further evaluation: CHEMBL2347006 and CHEMBL3970138. These analogs are in fact the same molecule despite slight differences in their SMILES representation. This molecule places within the top five candidates for highest probability of binding the target (shown in Supplementary Table 3), has the strongest predicted binding affinity, and places within the top five for lowest predicted BBB penetrance.

The AI scientist uses TOOLUNIVERSE to evaluate prior art in the patent literature for this candidate drug. It uses `PubChem_get_CID_by_SMILES` (API Tool) and `PubChem_get_associated_patents_by_CID` (API Tool) to retrieve URLs to drug-associated patents from PubChem. Then, it uses `get_webpage_text_from_url` (API Tool) to read the text of these patent URLs. Through this, the AI scientist discovered that the small molecule associated with CHEMBL2347006 and CHEMBL3970138 was already patented for use in cardiovascular disease in 2019 and 2021, revealing that another potential treatment for hypercholesterolemia nominated by the AI scientist was confirmed in the literature.

This case study demonstrates how TOOLUNIVERSE can be used to conduct flexible, multi-domain scientific research. It breaks out of the paradigm of a narrowly-focused bioinformatics pipeline; instead, the AI scientist leverages tools and data modalities across chemistry, human biology, and patent literature to retrieve multiple lines of evidence in supporting its final drug candidates.

References

1. Gao, S. *et al.* Empowering biomedical discovery with AI agents. *Cell* **187**, 6125–6151 (2024). URL <https://doi.org/10.1016/j.cell.2024.09.022>.
2. Boiko, D. A., MacKnight, R., Kline, B. & Gomes, G. Autonomous chemical research with large language models. *Nature* **624**, 570–578 (2023).
3. Swanson, K., Wu, W., Bulaong, N. L., Pak, J. E. & Zou, J. The virtual lab of ai agents designs new sars-cov-2 nanobodies. *Nature* 1–3 (2025).
4. Virshup, I. *et al.* The scverse project provides a computational ecosystem for single-cell omics data analysis. *Nature Biotechnology* **41**, 604–606 (2023).
5. Lobentanzer, S. *et al.* Democratizing knowledge representation with BioCypher. *Nature Biotechnology* **41**, 1056–1059 (2023).
6. Heumos, L. *et al.* An open-source framework for end-to-end analysis of electronic health record data. *Nature Medicine* **30**, 3369–3380 (2024).
7. Wratten, L., Wilm, A. & Göke, J. Reproducible, scalable, and shareable analysis pipelines with bioinformatics workflow managers. *Nature Methods* **18**, 1161–1168 (2021).
8. Gayoso, A. *et al.* A Python library for probabilistic analysis of single-cell omics data. *Nature biotechnology* **40**, 163–166 (2022).
9. Channing, G. & Ghosh, A. Ai for scientific discovery is a social problem. *arXiv:2509.06580* (2025).
10. Wang, H. *et al.* Scientific discovery in the age of artificial intelligence. *Nature* **620**, 47–60 (2023).
11. Anthropic. Introducing the model context protocol (2024). Anthropic blog, November 25 2024.
12. Yao, S. *et al.* React: Synergizing reasoning and acting in language models. In *International Conference on Learning Representations (ICLR)* (2023).
13. Gao, S. *et al.* TxAgent: An ai agent for therapeutic reasoning across a universe of tools (2025). URL <https://arxiv.org/abs/2503.10970>. 2503.10970.
14. Brown, T. *et al.* Language models are few-shot learners. In Larochelle, H., Ranzato, M., Hadsell, R., Balcan, M. & Lin, H. (eds.) *Advances in Neural Information Processing Systems*, vol. 33, 1877–1901 (Curran Associates, Inc., 2020).

15. Swanson, K., Wu, W., Bulaong, N. L., Pak, J. E. & Zou, J. The virtual lab: Ai agents design new sars-cov-2 nanobodies with experimental validation. *bioRxiv* 2024–11 (2024).
16. Wang, Z. *et al.* GeneAgent: self-verification language agent for gene-set analysis using domain databases. *Nature Methods* 1–9 (2025).
17. Dong, G. *et al.* Tool-Star: empowering llm-brained multi-tool reasoner via reinforcement learning. *arXiv:2505.16410* (2025).
18. Liu, W. *et al.* DrBioRight 2.0: an llm-powered bioinformatics chatbot for large-scale cancer functional proteomics analysis. *Nature Communications* **16**, 2256 (2025).
19. Shao, Z. *et al.* Deepseekmath: Pushing the limits of mathematical reasoning in open language models. *arXiv preprint arXiv:2402.03300* (2024).
20. Schulman, J., Wolski, F., Dhariwal, P., Radford, A. & Klimov, O. Proximal policy optimization algorithms. *arXiv preprint arXiv:1707.06347* (2017).
21. Schenone, M., Dančák, V., Wagner, B. K. & Clemons, P. A. Target identification and mechanism of action in chemical biology and drug discovery. *Nature chemical biology* **9**, 232–240 (2013).
22. Ren, F. *et al.* A small-molecule tnfr inhibitor targets fibrosis in preclinical and clinical models. *Nature Biotechnology* **43**, 63–75 (2025).
23. Lin, X., Li, X. & Lin, X. A review on applications of computational methods in drug screening and design. *Molecules* **25**, 1375 (2020).
24. Passaro, S. *et al.* Boltz-2: Towards accurate and efficient binding affinity prediction. *BioRxiv* 2025–06 (2025).
25. Swanson, K. *et al.* ADMET-AI: a machine learning ADMET platform for evaluation of large-scale chemical libraries. *Bioinformatics* **40**, btae416 (2024).
26. Botti, R., Triscari, J., Pan, H. & Zayat, J. Concentrations of pravastatin and lovastatin in cerebrospinal fluid in healthy subjects. *Clinical neuropharmacology* **14**, 256–261 (1991).
27. Wittmann, B. J. *et al.* Strengthening nucleic acid biosecurity screening against generative protein design tools. *Science* **390**, 82–87 (2025).
28. Tang, X. *et al.* Risks of AI scientists: prioritizing safeguarding over autonomy. *Nature Communications* **16**, 8317 (2025).
29. Guan, M. Y. *et al.* Deliberative alignment: Reasoning enables safer language models. *arXiv:2412.16339* (2024).

30. OpenAI. Introducing chatgpt agent: Bridging research and action. <https://openai.com/index/introducing-chatgpt-agent/> (2025).
31. Gemini CLI Contributors. gemini-cli: An open-source ai agent that brings the power of gemini directly into your terminal. <https://github.com/google-gemini/gemini-cli> (2025).
32. Claude code. <https://claude.com/product/claude-code> (2025).
33. QwenLM Contributors. Qwen code. <https://github.com/QwenLM/qwen-code> (2025).
34. LangChain Contributors. Langchain: A framework for developing language model applications. <https://github.com/langchain-ai/langchain>.
35. Deepset. Haystack: An open-source framework for building nlp-powered search systems. <https://github.com/deepset-ai/haystack> (2019).
36. Wu, Q. *et al.* Autogen: Enabling next-gen llm applications via multi-agent conversation framework. *arXiv preprint arXiv:2308.08155* (2023).
37. Li, G., Hammoud, H. A. A. K., Itani, H., Khizbullin, D. & Ghanem, B. Camel: Communicative agents for” mind” exploration of large language model society. In *Thirty-seventh Conference on Neural Information Processing Systems* (2023).
38. Shi, Z. *et al.* Tool learning in the wild: Empowering language models as automatic tool agents. In *Proceedings of the ACM on Web Conference 2025*, 2222–2237 (2025).
39. Wang, H., He, Y., Paula, C., Bucci, M. & other. Spatialagent: An autonomous ai agent for spatial biology. *bioRxiv* (2025). URL <https://www.biorxiv.org/content/early/2025/04/01/2024.04.01.646459>.
40. Targets, O. 24.09 platform release now live. <https://community.opentargets.org/t/24-09-platform-release-now-live/1556?ref=blog.opentargets.org> (2024).
41. Pearce, J. D. *et al.* A cross-species generative cell atlas across 1.5 billion years of evolution: The transcriptformer single-cell model. *bioRxiv* (2025). URL <https://www.biorxiv.org/content/early/2025/04/29/2025.04.25.650731>. <https://www.biorxiv.org/content/early/2025/04/29/2025.04.25.650731.full.pdf>.
42. Li, M. M. *et al.* Contextual AI models for single-cell protein biology. *Nature Methods* **21**, 1546–1557 (2024). URL <https://doi.org/10.1038/s41592-024-02341-3>.
43. DepMap, B. DepMap 24Q2 Public (2024). URL https://plus.figshare.com/articles/dataset/DepMap_24Q2_Public/25880521.